Juniper Networks
Intrusion Detection and Prevention

IDP Reporter User's Guide

Release 4.1r2a/4.1r3/4.2r1
September 2008

Contents

1. "Getting Started" on page 2
2. "Working with Dashboards and Reports" on page 8
3. "Using Global and Local Filters" on page 17
4. "Exporting Reports" on page 20
5. "Using Profiles to Generate Custom Reports" on page 21
6. "IDP Reporter Options" on page 27

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000

www.juniper.net

Part Number: 530-000000-01

1 Getting Started

IDP Reporter is a Java application that has been preinstalled on your IDP appliance.

IDP Reporter enables you to analyze your enterprise network thoroughly so you can assess attacks, attackers, and resource utilization.

IDP Reporter collects traffic logs from the IDP appliance, parses them, and presents them as reports in HTML, PDF, or text formats.

1.1 IDP Dependencies

Juniper Networks supports IDP Reporter on the following platforms:

- IDP 50/200/600/1100 (4.1r3)
- IDP 75/250/800 (4.1r2a or 4.1r3)
- IDP 8200 (4.2r1)

IDP Reporter provides reports of statistics gathered by IDP processes. In order to produce statistics, you must enable Application Volume Tracking (AVT) and run the Profiler.

To enable AVT:

1. Connect to the IDP command-line interface:
   - Use SSH to connect to the IP address or host name for the management interface. Log in as admin and switch to the user root (`su -u root`).
   - If you prefer, make a connection through the serial port and log in as the user root.
2. Run the following command to check if AVT is running on the sensor:

   ```
   scio const -s s0:flow get sc_periodic_stat_update
   ```

   If AVT is running, the console returns a message that sc_periodic_stat_update is set to 0x1. If it does not, continue.
3. Run the following command to enable AVT:

   ```
   scio const -s s0:flow set sc_periodic_stat_update 1
   ```

To start the Profiler:

1. In NSM, navigate to the NSM device manager.
2. Double-click the IDP device to display the edit device properties dialog box.
3. Click the **Profiler Settings** tab and ensure you have enabled profiler, application profiling, have selected tracked hosts, and have selected contexts. For information on these settings, see the NSM online Help.

4. To start the Profiler, select **Devices > IDP Profiler > Start Profiler**.

5. Select the IDP device.

6. Click **OK**.

1.2 Accessing the IDP Reporter User Interface

You can access the IDP Reporter user interface with the following browsers:

- Internet Exporer 6.x, 7.x
- Mozilla Firefox 2.x

NOTE: IDP Reporter does not support Mozilla Firefox 3.x.

To access the IDP Reporter user interface:

1. Download the latest Java virtual machine from the following location:

   http://www.java.com/en/download/index.jsp

2. Install the Java software on your client host.

3. Ensure you have enabled Java and JavaScript in your Web browser. Do not block pop-ups.

4. Type the following URL in your browser's Address box:

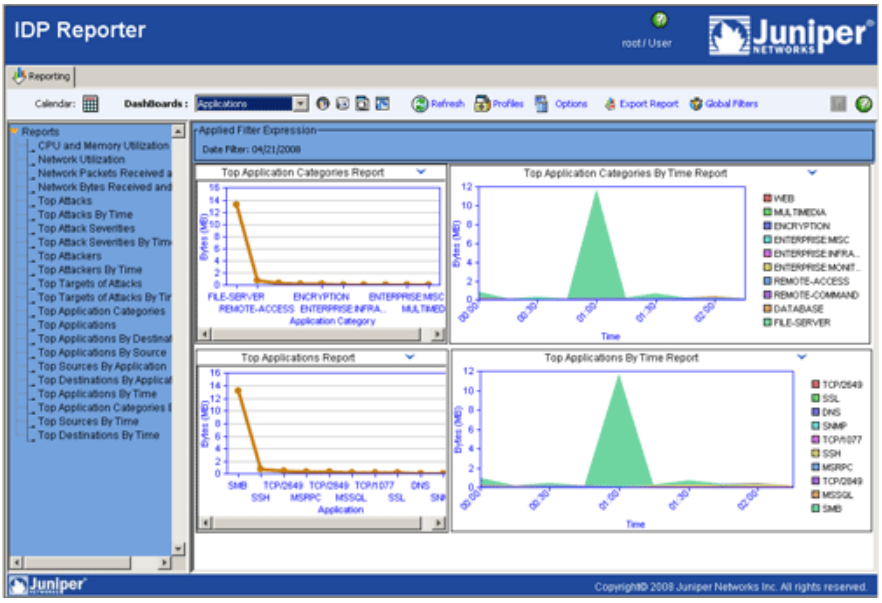
   https://*mgmt-port_PI-address*/reports

   Where *mgmt-port_PI-address* is the IP address for the management port on the IDP appliance.

5. Specify the credentials set for the Appliance Configuration Manager (ACM) when prompted for a user name and password.

The browser displays the IDP Reporter default dashboard, as shown in Figure 1.

Figure 1: IDP Reporter Default Dashboard



NOTE: If the IDP Reporter user interface does not appear, see Troubleshooting Access to the IDP Reporter User Interface on page 4.

1.3 Getting Help

Each page or dialog box includes a Help icon. Click the icon to display help for the page or dialog box.

For problem resolution, Juniper Networks has an online self-service portal called Customer Support Center (CSC). You can find it at http://www.juniper.net/customers/support.

1.4 Troubleshooting Access to the IDP Reporter User Interface

You can access IDP Reporter with any browser that supports Java Virtual Machine. IDP Reporter requires a specific version of the Java Runtime Environment (JRE). If you do not already have this Java plug-in, IDP detects this and prompts you to install the compatible version. Follow the prompts to download and install the specific version from Sun Microsystems.

Resolving Errors Due to Browser Settings

In your browser, you must enable Java and JavaScript and allow pop-ups.

Resolving Warnings or Errors Due to JRE Maximum Heap Space Settings

We recommend you set the JRE maximum heap space to 256 MB. If your heap space is between 128 MB and 256 MB, IDP Reporter can be launched but displays a message noting the recommended heap space. If the heap space is set to less than 128 MB, IDP Reporter cannot be launched.

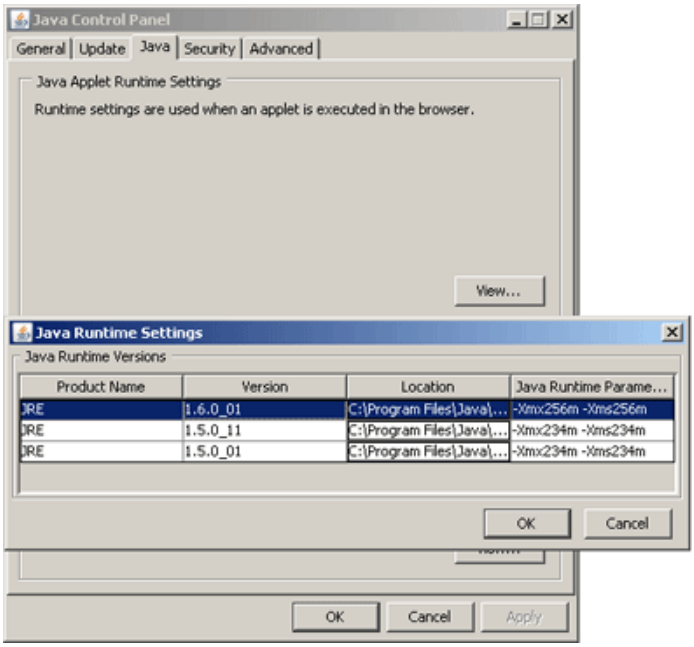
To set the JRE maximum heap space:

1. Click **Start > Control Panel > Java** to display the Java Control Panel.
2. Click the **Java** tab.
3. Click the **View** button in the Java Applet Runtime Settings area.
4. Click the cell in the Java Runtime Parameters column and type the following values:

   ```
   -Xms256M -Xmx256M
   ```

   Figure 2 shows an example of Java Control Panel JRE heap space settings.

Figure 2: Java Control Panel JRE Heap Space Settings



Eliminating Certificate Warnings

When you access the IDP Reporter, you might encounter warning messages indicating that a certificate authority cannot be verified or a site certificate does not match hostname.

To eliminate these warnings:

1. Click **Start > Control Panel > Java** to display the Java Control Panel.
2. Click the **Advanced** tab.
3. Clear the following options under the Security section:
   - Warn if certificate authority cannot be verified
   - Warn if site certificate does not match hostname

Restarting the IDP Reporter Service

If you encounter an issue where the IDP Reporter service is unreachable, you might need to restart the service.

To restart the service:

1. Connect to the host using SSH and log in as the administrator.
2. Run the following command:

   /etc/init.d/idprepservice restart

1.5 Troubleshooting Statistics Collection

If IDP Reporter reports do not show statistics:

- Ensure you have enabled AVT and started Profiler.

  See "IDP Dependencies" on page 2.

- Ensure the IDP process is up and running:

  1. Connect to the IDP command-line interface:

     - Use SSH to connect to the IP address or host name for the management interface. Log in as admin and switch to the user root (`su -u root`).
     - If you prefer, make a connection through the serial port and log in as the user root.

  2. Run the following command:

     idp.sh status

  3. Restart the process if needed.

- Ensure the IDP appliance is generating AVT files:

  1. Connect to the IDP command-line interface:

     - Use SSH to connect to the IP address or host name for the management interface. Log in as admin and switch to the user root (`su -u root`).
     - If you prefer, make a connection through the serial port and log in as the user root.

  2. Navigate to /usr/idp/device/var/stat/ and check the timestamps for AVT files.
  3. Run the following command:

     statview meta

The console displays data about latest AVT collection.

4. If the history shows collection stopped at some point, review your AVT and Profiler settings. See “IDP Dependencies” on page 2.

- Review IDP Reporter log messages in the following locations:

  - /var/idp/reporter/logs/
  - /usr/idp/reporter/diaglogs/mainengine.log
  - /usr/idp/reporter/diaglogs/Parserdiag.log

  If logs indicate IDP Reporter has stopped or is in a problematic state, restart it with the following command:

  /etc/inet.d/idprepservice [start|stop|restart]

- If data collection is functioning but you do not see expected statistics in particular reports, check your IDP Reporter filter settings.

  Try removing filters to validate statistics are generated for a particular report. Then reapply filters and verify the report data has changed to reflect the logic of the filter.

  See “Configuring Global Filters” on page 17 and “Applying Local Filters” on page 17.

2 Working with Dashboards and Reports

A *dashboard* contains a set of reports that are populated by queries of IDP appliance logs.

The default IDP Reporter dashboard includes the following reports:

- CPU and Memory Utilization
- Network Utilization

The Dashboards drop-down list contains the default and user-created dashboards.

Table of Contents Frame

The table of contents frame, shown in Figure 3, displays a hierarchy of reports. At all levels of the hierarchy, related queries are grouped together.

Figure 3: Table of Contents Frame

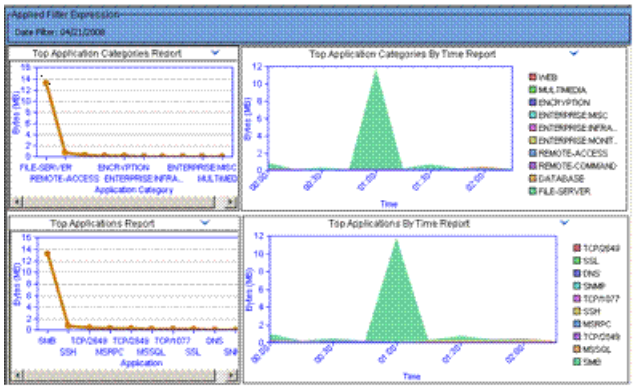
To expand or collapse a group of reports, click the arrow to the left of the group name.

To display a report in the report frame, click the report name.

Report Frame

The report frame, shown in Figure 4, displays either the reports configured for the active dashboard or a report selected from the table of contents frame.

Figure 4: Report Frame


Top Application Categories Report
Top Application Categories By Time Report
Top Applications Report
Top Applications By Time Report

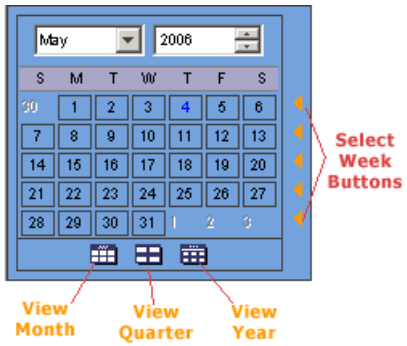
All reports include a title, a short description at the bottom of the frame, identification of filters that have been applied (such as a date filter or global filter), and a table or graph of results.

Report attributes are color-coded for easy comparison and analysis. A graph legend defines the color-coding.

Calendar Frame

The calendar frame, shown in Figure 5, enables you to apply time filters across reports.

Figure 5: Calendar Frame



To display the calendar frame, click the Calendar icon.

Select a month and year from the top of the calendar.

Shift-click to select a contiguous date range. Ctrl-click to select noncontiguous days.

Use the Select Week buttons along the right-side of the calendar to select the corresponding week.

Use the View Month, View Quarter, and View Year buttons along the bottom to select the corresponding interval.

NOTE: If you apply View Quarter or View Year date filters, you cannot use the Query by Day filter.

NOTE: When the report frame displays dashboard reports, the Calendar icon appears dimmed and unavailable.

Applied Filter Expression

Data filters that have been applied to a report are listed under the report title. There are three types of filters:

- **Date Filter**—The date filter displays the date, month, and year when the report data was collected. You can use the calendar frame to display data for different dates. See Calendar Frame on page 9.
- **Global Filter**—Global filters take precedence over local filters in the report. To display global filters, click the **Global Filter** icon. To disable global filters, click the **Local Filter** icon and select the **Disable Global Filters** check box. See Configuring Global Filters on page 17.
- **Local Filters**—You apply local filters to refine results after you see an initial version of the report. From the report of interest, click the **Local Filter** icon to display the Local Filters dialog box. Select the **No filter** check box to disable all filters on the displayed report. Local filters are applicable only when the global filters are disabled. Select the **Disable Global filters** check box to disable them. See Applying Local Filters on page 17.

Report Utilities

IDP Reporter includes utilities to modify or make use of reports. You access some tools by clicking icons and others with the right-click context menu. Tools are available and displayed only when relevant. Table summarizes these tools.

Table 1: Summary of Report Utilities

Utility Icon/Name	Description
Options	Displays the Options dialog box. See IDP Reporter Options on page 27.
Export Report	Displays the Export Report dialog box. See Exporting Reports on page 20
Profiles	Displays the Profile Manger. See Using Profiles to Generate Custom Reports on page 21.
Global Filters	Displays the Global Filters dialog box. See Global Filters on page 17.

Table 1: Summary of Report Utilities (continued)

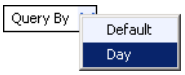
Utility Icon/Name	Description
Local Filter	Displays the Local Filters dialog box. See Applying Local Filters on page 17.
Display/Hide Filter List	Shows or hides the applied filters. This icon is visible only when filters are applied on this query.
Snap	Displays a snapshot of the active report in a new browser window.
Export to PDF	Exports the active report to a PDF file. Internet Explorer settings for opening a PDF Report: Click **Tools > Internet Options > Advanced Settings > Security** and clear the **Do not save encrypted pages to disk** check box for the PDF reports to open upon exporting them.
Show/Hide Graph	Hides or shows a graph. By default, the report frame is divided in two: a graph in the upper region and a table in the lower region.
Refresh	Refreshes data in the active report.
Help	Displays online Help for the window or dialog box.
Query By 	Toggles between By Default or By Day. Note: The Query By Day option cannot be applied in conjunction with the View Quarter or View Year date filters from the calendar.
Graph Type	Selects a graph type from among the following formats: ■ Bar ■ Pie ■ Tape ■ Horizontal ■ Area ■ Stacked Horizontal ■ Stacked Vertical ■ More If you select **More**, a new window appears where you can select Bar, 3DBar, 2DLine, 3DLine, 2DArea, 3DArea, Horizontal, Radar, Gauge, PIE, and 3DPIE. Available types depend on the kind of data available for that query. For single row data, only line graph can be displayed irrespective of the graph option selected.

Table 1: Summary of Report Utilities (continued)

Utility Icon/Name	Description
Show Legend	Shows graph legends. Graph legends are a key to the data plotted on the graph. For pie charts, the graph legend is shown only if the number of records present in the selected query are fewer than 24. For other graph types, the graph legend is shown only if the number of entries of data elements related to the selected query are fewer than 12.
No. Records and No. Subrecords	Specifies the maximum number of records and subrecords that you want to view in your selected report.
Include Trends	Records the trend of specific current and previous events happening at the devices. Trends show the number of times a particular event type occurred over a period of time. When you include trends, IDP appends the report with the following columns: ■ Today's Count ■ Yesterday's Count ■ Last Seven Days ■ Current Month
Reporting Drilldown	Redisplays the instant report and populates related reports in the table of contents frame with similarly filtered views of the reports. Report tables contain records of network events, including columns of attributes. To filter the report by attribute, right-click an attribute in the table record and select **Reporting Drilldown**.
Workbench	Shows the reporting values for the single event. Report tables contain records of network events. To display the Workbench page for the event, right-click the record in the report table and select **Workbench**.
WHOIS	Displays the WHOIS report for the IP address. If a report record includes an IP address attribute, you can right click and select **WHOIS**.

2.1 Creating a Custom Dashboard

A *dashboard* is a user interface that organizes and presents complex information in a way that is easy to comprehend.

The dashboard management tools, shown in Figure 6, include a drop-down list of default and user-created dashboards, as well as toolbar button utilities to create new dashboards, change the default dashboard, copy dashboard objects, and toggle to dashboard design mode.

Figure 6: Dashboard Management Tools

Table 2 summarizes these tools.

Table 2: Summary of Dashboard Management Tools

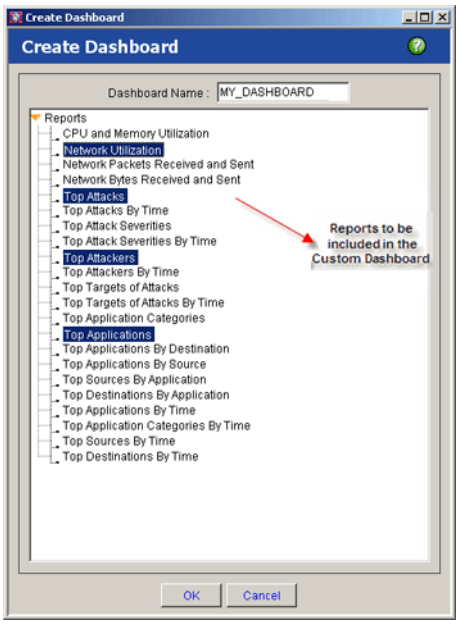
Utility Icon/Name	Description
Create New Dashboard	Creates customized dashboards.
Set Current Dashboard as Default	Sets the custom dashboard that you created to display the information you need most and would want to monitor regularly as the default view.
Restore Factory Default View.	Restores the factory default view.
Delete Dashboard	Deletes the active dashboard
Copy Dashboard	Saves a copy of the current dashboard. By default, the name of the copy is Copy_of_*dashboard-name*. You can enter the name of your choice in the dialog box.
Toggle Design/Run Mode	Toggles between design mode, where you can customize the look-and-feel and content of dashboard panels, and run mode, where you display reports.

2.2 *Adding Dashboards*

To add a new dashboard:

1. Click the **Create New Dashboard** icon to display the Create Dashboard dialog box. See Figure 7.

Figure 7: Create Dashboard Dialog Box



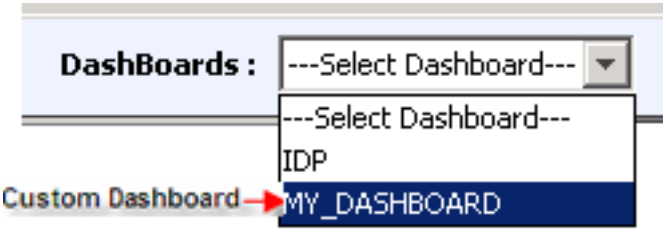
2. Type a name in the Dashboard Name box. For example, type **MY_Dashboard**.

3. Use Shift-click and Ctrl-click to select the report titles that you want to see in the new dashboard. Click **OK**.

   The dashboard is saved and displayed in the DashBoards drop-down list.

4. Select MY_DASHBOARD from the DashBoards list to display the new dashboard.

Figure 8: DashBoards List



To set this dashboard as your default selection, select the dashboard from the list and click the Set **Current Dashboard as Default** icon.

To return to the factory default dashboard, click the **Restore Factory Default View** icon.

2.3 Redesigning Dashboard Panels

You can customize the layout of default and user-created dashboards. In design mode, you can resize, modify, delete, and add panels.

To activate design mode, click the **Toggle Design/Run Mode** icon.

Design mode reveals the following dashboard design tools.

Table 3: Summary of Design Mode Tools

Utility Icon/Name	Description
Add a Panel	Displays the Add Dashboard Panel dialog box. You can add both device-based and host-based panels to the dashboard.
Save Dashboard	Saves changes you have made in design mode.
Layout Design Tools ■ Resize width ■ Resize height ■ Resize both ■ Left align ■ Right align ■ Top align ■ Bottom align	To change panel properties with a layout design tool: 1. Hold the Ctrl key and click the panels that you want to resize or realign. 2. Continue to hold the Ctrl key and click the panel that you want to use as a model. 3. Click the desired tool. For example, click **Resize width**. All panels are resized according to the width of the last panel selected.
Panel Menu	Displays a menu of tools you can use to modify panel content. See Modifying Panel Content on page 16.

NOTE: If your current selection is the default dashboard, then the Set Current Dashboard as Default icon appears dimmed and unavailable. You cannot resize or realign the panels on the default dashboard.

2.4 Adding a Panel to a Dashboard

Dashboards are composed of a number of panels. A *panel* includes a report and utilities to customize and make use of the report.

To add panels to your dashboard:

1. Click the Add Panel icon to display the Add Dashboard Panel dialog box.
2. Select the desired report.
3. Click **OK**.

2.5 Modifying Panel Content

To modify panel content:

1. Click the Panel Menu icon that appears near the panel report title to display panel design menus.

2. Use the Panel Menu utilities to customize the panel content. Table 4 describes these utilities.

Table 4: Panel Menu Utilities

Utility Icon/Name	Description
Panel Menu	Displays a menu of tools you can use to modify panel content. The Panel Menu icon appears on each panel next to the panel report title.
Zoom	Displays the panel in a new browser window.
Snap	Displays a snapshot of the active panel in a new browser window.
Modify Report Contents	Displays the Modify Dashboard View dialog box, where you select a report to appear in the panel.
Display Type	Sets a graph type from among the following formats: ■ Bar ■ Pie ■ Tape ■ Horizontal ■ Area ■ Stacked Horizontal ■ Stacked Vertical ■ More If you select **More**, a new window appears where you can select Bar, 3DBar, 2DLine, 3DLine, 2DArea, 3DArea, Horizontal, Radar, Gauge, PIE, and 3DPIE. Available types depend on the kind of data available for that query. For single row data, only line graph can be displayed irrespective of the graph option selected.
Show Legend	Includes graph legends. Graph legends are a key to the data plotted on the graph. For pie charts, the graph legend is shown only if the number of records present in the selected query are fewer than 24. For other graph types, the graph legend is shown only if the number of entries of data elements related to the selected query are fewer than 12.
Local Filter	Displays the Local Filters dialog box. See Applying Local Filters on page 17. **Note**: The Local Filters utility is visible only when there are supported filter elements; reports must contain at least one column on which the report can be filtered.

3 Using Global and Local Filters

This section describes how to work with global filters and local filters.

3.1 Configuring Global Filters

You use global filters to set filters uniformly across the queries that generate IDP Reporter reports.

To configure global filter settings:

1. Click the **Global Filters** button from the main window to display the Global Filters dialog box.

NOTE: This same procedure applies when you access the Global Filters dialog box from the Export Reports utility.

2. Specify a number of records and subrecords to be displayed in the report.

3. Configure filter elements. You can configure filter that include matching results and filters that exclude matching results. Table 5 provides the column ID and a brief description for each global filter.

Table 5: Global Filters

Filter Name	Column ID	Description
Application Category	Application Category	Application category filter
Description	desc	Description filter
Application	Application	Application filter
Destination	Destination	Device destination filter
Event Code	Event Code	Code filter
Source	Source	Source IP filter
Hour	hod	Hour of day filter

4. Click **Save**.

3.2 Applying Local Filters

You use local filters to broaden or narrow the scope and number of records displayed. You can also use filters to change the graph type.

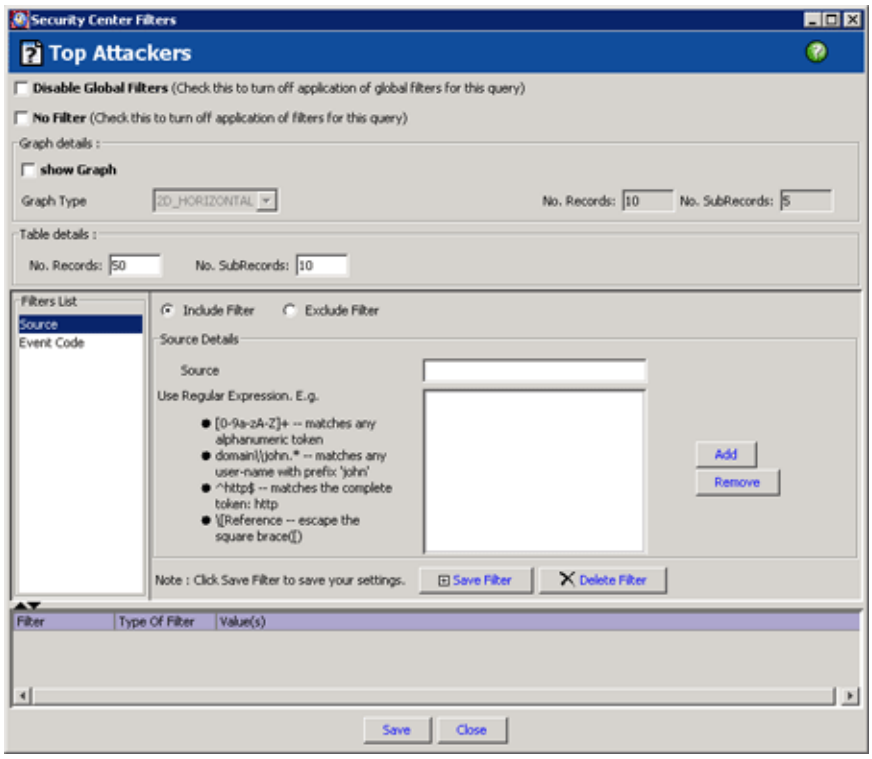
By default, global filters are applied to each query.

To specify local filters:

1. Click a report title in the table of contents frame to display the report in the report frame.

2. Click the **Local Filter** icon to display the Local Filters dialog box. See Figure 9.

Figure 9: Local Filters Dialog Box



3. Select the **Disable Global Filters** check box.

4. Optionally, select the **No Filter** check box to negate all the filters applied on this query.

5. Specify whether to show the report in graph form.

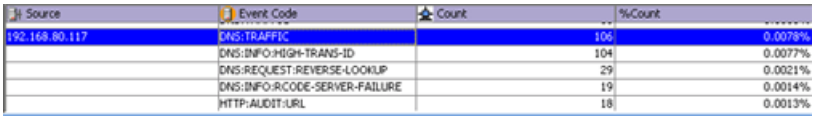
NOTE: Not all reports are associated with graphs.

6. Specify a maximum number of records and subrecords to display.

7. Add a number of filters according to the following example.

   Example: Suppose you have generated a event report that displays event code DNS:TRAFFIC.

Figure 10: Local Filter Example



Source	Event Code	Count	%Count
192.168.80.117	DNS:TRAFFIC	106	0.0078%
	DNS:INFO:HIGH-TRANS-ID	104	0.0077%
	DNS:REQUEST:REVERSE-LOOKUP	29	0.0021%
	DNS:INFO:RCODE-SERVER-FAILURE	19	0.0014%
	HTTP:AUDIT:URL	18	0.0013%

   If you do not want records with this event code included in the report, you can define an Exclude filter to exclude such events.

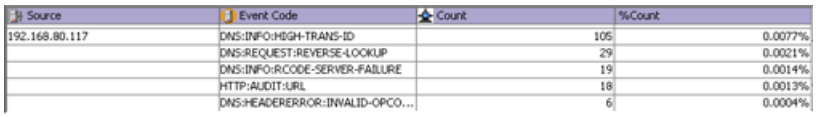
   a. Specify the source details.

   b. Select **Event Code** from the filters list and specify the event code that is to be excluded.

c. Click **Save Filter** to save the settings.

d. After the filter is applied, the report excludes records for the DNS:TRAFFIC event codes generated from the selected device.

Figure 11: Local Filter Example



Source	Event Code	Count	%Count
192.168.80.117	DNS:INFO:HIGH-TRANS-ID	105	0.0077%
	DNS:REQUEST:REVERSE-LOOKUP	29	0.0021%
	DNS:INFO:RCODE-SERVER-FAILURE	19	0.0014%
	HTTP:AUDIT:URL	18	0.0013%
	DNS:HEADERERROR::INVALID-OPCO...	6	0.0004%

Observe the following guidelines when you use regular expressions in filters:

- To filter the regular expression as it is in the reports, add the prefix ^ (caret symbol) and suffix $ (dollar symbol) before and after the regular expression. For example, if you want to filter event code 8690, enter **^8690$** in the regular expression text box to display identical event codes in the report. Without these symbols, all the event codes that contain 8690 in them will be displayed.

- To filter event attributes, use the caret symbol (^) as a prefix to any regular expression that starts with the common value as entered in the regular text box. For example, if you want to filter all the event codes starting with 193, enter **^193** in the regular expression text box to display all the event codes starting with 193 in the report. Without these symbols, all the event codes that contain 193 anywhere in them will be displayed.

- To specify a range to be filtered in the report, like 30-40 KB, use the prefix \ (backslash symbol) before the - (hyphen). For example, if you want to consider all events that recorded bandwidth in the 30-40 KB range, type **30\-40 KB**, and all the events that fall within the 30-40 KB bandwidth range will be displayed in the instant report.

- To filter an expression that contains a comma (,) in it, specify a dot symbol (.) instead of a comma in the regular expression.

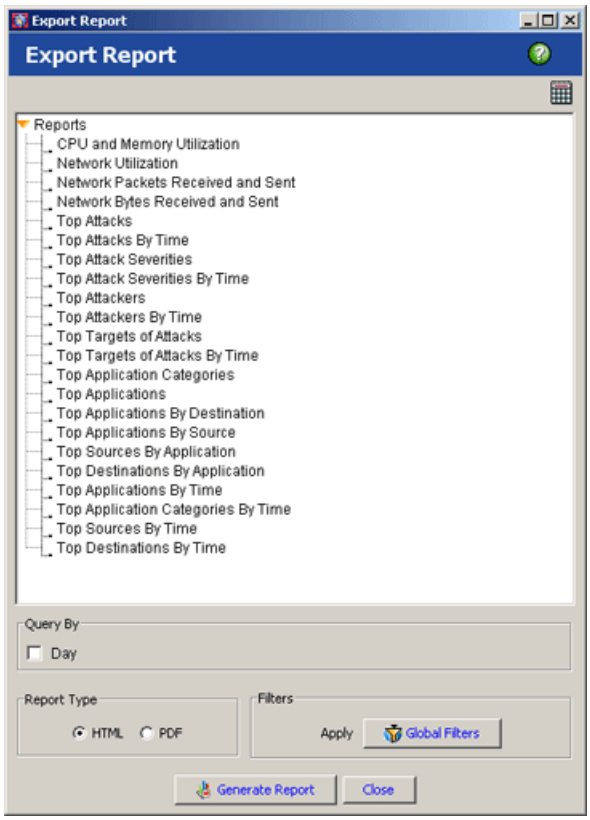
4 Exporting Reports

You can export reports into PDF or HTML files.

To export a report:

1. Click the Export Report icon in the taskbar to display the Export Report dialog box. See Figure 12.

Figure 12: Export Report Dialog Box



2. Under Query By, clear the Day check box to query by default, or select Day to include an aggregation by day.

3. Under Report Type, select **HTML** or **PDF.**

NOTE: If you export PDF reports, you must ensure the following browser setting is not selected. Click **Tools > Internet Options > Advanced Settings > Security**. Clear the **Do not save encrypted pages to disk** check box.

4. Under Filters, click the **Global Filters** button to display the Global Filters dialog box. Define the filters to be applied in the reports. See Configuring Global Filters on page 17.

5. Click **Generate Report** to export the report.

5 Using Profiles to Generate Custom Reports

A *profile* is an object that defines the schedule for log collection jobs, as well as data filters, report types, and delivery information for custom reports. Once created, you can use the profile to generate reports whenever necessary.

You can use the Profile Manager to create, edit, copy, and delete profiles.

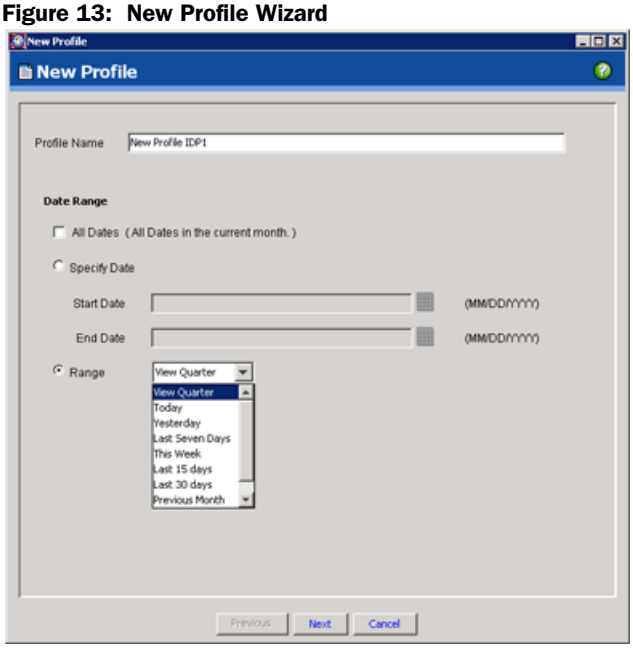
5.1 Creating a New Profile

To create a profile:

1. Click the **Profiles** icon in the taskbar to display the Profile Manager.

2. Click **New Profile** to display the first page of the New Profile wizard. See Figure 13.

Figure 13: New Profile Wizard



a. Specify a unique name in the Profile Name box.

b. Configure the date range for data using one of the following options:

- Select **All Dates** to include events from all dates in the current month.
- Select **Specify Date** and specify a start date and an end date to set a specific date range.
- Select **Range** and select one of the following predefined periods:
  - View quarter
  - Today
  - Yesterday

- Last seven days
- This week
- Last 15 days
- Last 30 days
- Previous month
- This month

c. Click **Next** to display the Scheduler and Filter Template page of the New Profile wizard.

3. Select a task from or create a new one, if necessary.

   To create a new task:

   a. Click the **Add** button.

   b. Select the frequency at which you want the profile to run.

   c. Specify a unique name in the Task Name box. This name is displayed among scheduled tasks.

   d. Select the frequency from the options given in Table 6.

Table 6: Frequency Options

Frequency	Description
Hourly	Select the **Hour** options button to schedule the task on an hourly basis and to specify the interval. The start time is specified in the Start Time edit box. To schedule a task by hour: 1. Specify the time at which you want the scheduled task to start. The current time is displayed in the format hh:mm:ss by default. To change it, specify a different time value in the text box. For example, type **13:49:37**. 2. Specify the day you want the scheduled task to start. Use the Calendar button to select the start date. 3. Specify the interval at which you want the scheduled task to start. The intervals are 1, 3, 6, and 12 hours. Click **Finish**.
Daily	Select the **Daily** options button to schedule the task on a daily basis and to specify the time. You can also select to perform on weekdays. The start time is specified in the Start Time edit box. The scheduled reports will not be generated before this time. To schedule a task by day: 1. Specify the time at which you want the scheduled task to start. The current time is displayed in the format hh:mm:ss by default. To change it, specify a different time value in the text box. 2. Specify the day you want the scheduled task to start. Use the Calendar button to select the start date. 3. Specify whether you want to schedule the task everyday or on weekdays and click **Finish**.

Table 6: Frequency Options (continued)

Frequency	Description
Weekly	Select the **Weekly** options button and click **Next** to display a dialog box where you can select the days of the week and the start time. This will result in the scheduled job being performed on the selected days of the week. The start time is specified in the Start Time edit box. The scheduled reports will not be generated before this time. Type in the time at which you want the scheduler to begin scheduling IDP Reporter jobs. To schedule a task by week: 1. Specify the time at which you want the scheduled task to start. The current time is displayed in the format hh:mm:ss by default. To change this, enter a different value in the text box. For example, type **18:24:30**. 2. Select the days of the week on which you want the scheduled tasks to run and click **Finish**.
Monthly	Select the **Monthly** options button and click **Next** to display a dialog box where you can select the month, start date, and the day of each month that you want to generate the report. You can also generate the report of a specific day of the week of each month. To schedule a task on a monthly basis: 1. Specify the time at which you want the task to start. The current time is displayed in the format hh:mm:ss by default. To change this, specify a different value in the text box. 2. Specify the date on which you want the task to start. To change this, use the Calendar button to specify a different value in the text box. 3. Click the **Day** options button to choose the day of the selected months on which you want the task to run or the **Every** options button to choose the day of the week of the selected months on which you want the task to run. 4. Select the months of the year in which you want the task to run and click **Finish**.
One Time Only	Select the **One Time Only** options button and click **Next** to display a dialog box where you can select the start time and start date when you want to generate the report. The start time is specified in the Start Time edit box. The scheduled reports will not be generated before this time. To schedule a one time task: 1. Specify the time at which you want the scheduled task to run. To change this, specify a different value in the text box. 2. Specify the day on which you want the scheduled task to run. Use the Calendar button to specify the start date and click **Finish**.

e. Click **Save**.

The schedule you just created is added to the list of scheduled tasks.

3. Select a filter template or create a new one, if necessary.

To create a new filter template:

a. Type a descriptive name in the Template Name box. Make sure this name is easy to remember and describes the data you are trying to filter.

b. Specify a number of records and subrecords to be displayed in the report output.

c. Add filters to the Filter List.

d. Click **Save Filter** to add the filter to the list.

e. Select a filter template and click **Next**.

4. Complete the following report style settings according to the procedures in Table 7.

Table 7: Report Style Settings

Setting	Procedure
Format	Select **HTML Report**, **PDF Report**, or **Text Report**. If you select **PDF Report**, you must ensure the following browser setting is not selected. Click **Tools > Internet Options > Advanced Settings > Security**. Clear the **Do not save encrypted pages to disk** check box.
Template	Select from a number of preconfigured report styles that have different fonts and colors or create and select a new template. Preconfigured styles include Cool, Vintage, Cascade, Serene Arcade, Sand Ribbon, Wise Monk, Capri Blue, Glass Block, Trendy, Standard, and Orange Spice. Template options are applicable for HTML reports only. To create a new template: 1. Click **Create**. 2. Select a background color and query color. 3. Click **Save**.
Organization	Specify the company name to appear in the report.
Logo File	Specify the absolute path to the logo file to be displayed in a report. The default path is *Installation Directory*\xhtmlfiles\logo.gif. To display a different logo, replace this image with your logo or specify a different absolute path.
Query By	Select **Day** to include a column that gives the details of the day when that particular event occurred.

Click **Next**.

4. Specify a number of report records and subrecords to appear in report tables. You can specify between 10 to 5000 records and between 1 to 500 subrecords.

5. Select a report template or create one, if necessary.

To create a report template:

a. Click **New Report**.

b. Specify an appropriate name in the Report Name box.

c. Use controls in the Selected and By Day columns to select queries and the By Day aggregation (if desired).

d. Click **Save** to add the report template to the template list.

e. Select a report template and click **Next**.

6. On the final wizard page, complete destination and distribution details, as described in Table 8. Click **Finish** to save the profile and exit the wizard.

Table 8: Completing Report Destination and Distribution Details

Destination	Procedure
Save As	To configure the location where reports are generated: 1. Click **Grammar** to display the Grammar dialog box. 2. Use the **Browse** button to set the report path. The path for the folder you select appears in the Report Path box. 3. Specify a prefix for report filenames in the Prefix box. 4. Follow the "Nomenclature for date format" shown in the dialog box to specify a date variable in the Date Format box. Note: Output files will be distinguished by the date format variable. For example, suppose you specify a prefix **IDP** and a date format **%m%%d%%y%**. Suppose further that the profile is scheduled to produce a daily report in HTML format. On June 21, 2008, IDP Reporter would generate a report with filename IDP062108.htm. On June 22, 2008, IDP Reporter would generate a report with filename IDP062208.htm. 5. Click **Set**.
E-mail Distribution	To configure e-mail distribution for generated reports: 1. Select the **Mail To** box 2. Specify an email address in the corresponding text box. To send e-mail to multiple recipients, use commas to separate the e-mail addresses. 3. Specify a subject line. 4. Configure Simple Mail Transfer Protocol (SMTP) settings: a. Click **Configure SMTP** to display the SMTP settings dialog box. b. Specify the fully qualified domain name of your SMTP server. c. Specify the user name of the authorized user with administrative rights to access the mail server. d. Select **SMTP Server requires authentication** if appropriate. If your SMTP server requires authentication, select the option button and click **Settings** to display a dialog box for authentication settings. e. Optionally, specify your email address and click Send Test Mail to verify proper configuration.
FTP Distribution	To transfer reports using FTP: 1. Select the FTP check box and enter the host name, user name, and password. (The host machine must be running the FTP service.) 2. Optionally, select the Passive Mode check box if you want IDP Reporter to use passive FTP to initiate FTP connections. Passive FTP connections provide more security for the network that hosts the FTP server to which IDP Reporter will connect. Clients that use passive FTP send a PASV command, which allows the server to specify which data port it wants to use, rather than sending a standard POST command to specify a control channel and data channel port.

5.2 Editing a Profile

To edit a profile:

1. Click the **Profiles** icon in the taskbar to display the Profile Manager.
2. Click **Edit Profile** to display the Edit Profile wizard.
3. Use the tabs and controls to modify the configuration settings as needed. See Creating a New Profile on page 21 for details on completing the configuration.
4. Click **Save**.

5.3 Copying a Profile

To copy a profile:

1. Click the **Profiles** icon in the taskbar to display the Profile Manager.
2. Select an existing profile.
3. Click **Copy Profile**.

   The Copy Profile window displays the newly created profile which is identical to the former profile except for the profile name.

5.4 Deleting a Profile

To delete a profile:

1. Click the **Profiles** icon in the taskbar to display the Profile Manager.
2. Select a profile and click **Delete Profile**.

6 IDP Reporter Options

You can modify a few product settings in the Options dialog box.

To display product options, click the **Options** icon in the taskbar.

6.1 Language Settings

By default, IDP Reporter parses English language logs. Use the Options dialog box to specify another supported language, including:

- Chinese
- Chinese (Traditional)
- Japanese
- Korean

6.2 Syslog Settings

If you have configured your IDP appliance to write to a syslog server, you can set the following additional options:

- **Send Attack Events —** Sends the collected attack events to an external recipient. Specify the following settings:
  - IP address of the client where the attack events are to be forwarded
  - Port number
- **Create Binary Delta —** Converts the data collected by the syslog into delta files.